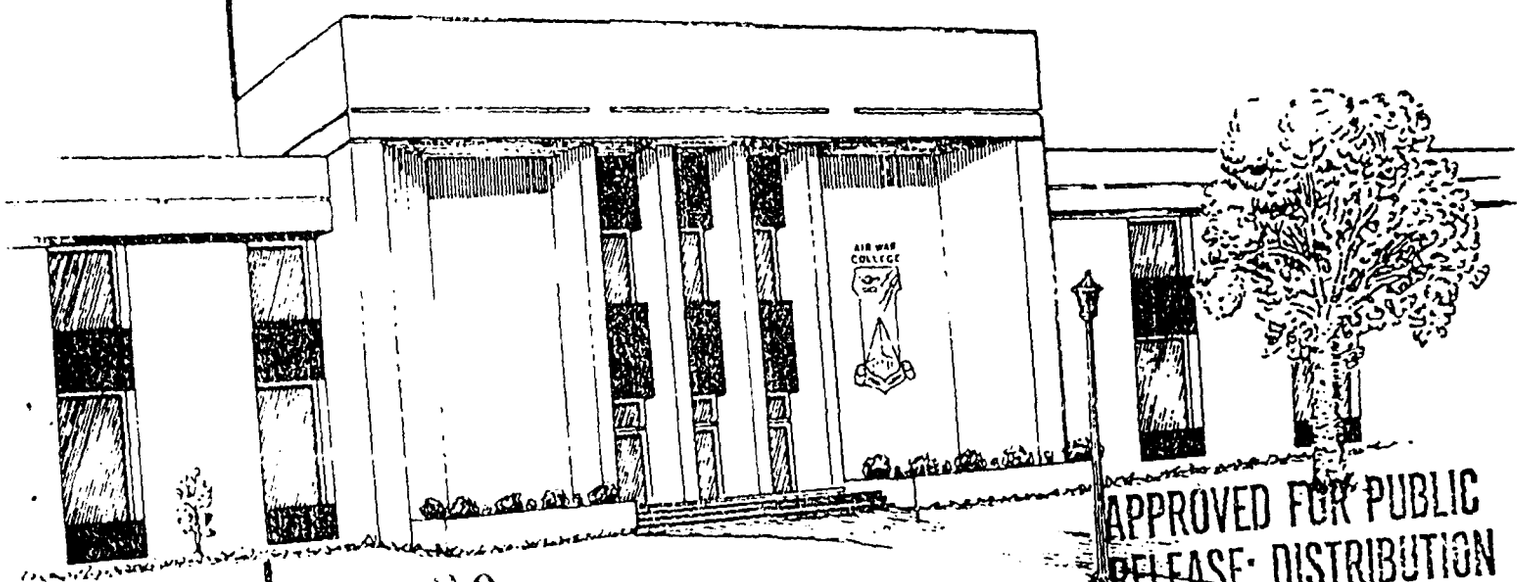
AIR WAR COLLEGE

RESEARCH REPORT

INFORMATION WAR

LIEUTENANT COLONEL MARK C. LEWONOWSKI

1991



30

AIR UNIVERSITY
UNITED STATES AIR FORCE
MAXWELL AIR FORCE BASE, ALABAMA

AIR WAR COLLEGE

AIR UNIVERSITY

INFORMATION WAR

by

Mark C. Lewonowski
Lieutenant Colonel, USAF

AN ESSAY SUBMITTED TO THE FACULTY

IN

FULFILLMENT OF THE CURRICULUM

REQUIREMENT

Advisor: Dr Charles H. Davis IV

MAXWELL AIR FORCE BASE, ALABAMA

April 1991

DISCLAIMER

This essay represents the views of the author and does not necessarily reflect the official opinion of the Air War College or the Department of the Air Force. In accordance with Air Force Regulation 110-8, it is not copyrighted but is the property of the United States government.

Loan copies of this document may be obtained through the interlibrary loan desk of Air University Library, Maxwell Air Force Base, Alabama 36112-5564 (telephone (205) 953-7223 or DSN 493-7223).

ABSTRACT

TITLE: Information War

AUTHOR: Mark C. Lewonowski, Lieutenant Colonel, USAF

The struggle to dominate the information sphere, the domain of command, control, communications and intelligence (C^3I), will be the center of gravity of future conflicts between modern forces. Command is an information function. The modern staff, and the data processing and communication systems it relies on, performs important value-adding analysis and decision services to aid the commander. The entire information system supporting the commander is essential to conducting modern warfare, and is, therefore, a critical target to be attacked and a vital resource to be protected.

For these reasons, the principles of information war must see specific application in United States force development strategies, and they must be integrated into the body of doctrine underlying our force employment strategies. Information and weapon technologies are maturing to the point that the ability to identify and locate a target in space and time implies the ability to destroy it. Modern weapons are dependent upon accurate, precise, and timely targeting information. Identifying and locating targets are critical intelligence functions. There are a number of active and passive measures available to defeat the enemy's targeting process.

BIOGRAPHICAL SKETCH

Lieutenant Colonel Mark C. Lewonowski (B.S., U.S. Air Force Academy; M.S., The George Washington University) has served as both a communications systems officer and as an intelligence officer in a variety of assignments throughout the Air Force. His most recent assignments include the Office of the Assistant Chief of Staff, Intelligence, Headquarters, U.S. Air Force; and a tour as Commander, 3480th Technical Training Group, Goodfellow Air Force Base, Texas. Colonel Lewonowski is a graduate of Squadron Officer School, the Armed Forces Staff College, and the Air War College, class of 1991.

TABLE OF CONTENTS

CHAPTER I

INFORMATION WAR

> Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.
>
> Air Marshal Giulio Douhet

The struggle to dominate the information sphere, the domain of command, control, communications and intelligence (C^3I) will be the center of gravity of future conflicts between modern forces. This essay is a discussion of principles of information war in a context of classical strategic theory and the principles of war. An understanding of the principles of information war must confirm the centrality of the information battle in future conflict.

Recent periods in world history have been variously characterized as the industrial age, the electronic age, the nuclear age, etc. We are now in the information age. That title reflects the fact that the dominant technology in the world today is information science, which in turn is based on a body of information theory, and includes technologies of sensor, information-processing, and communication systems.

Throughout human history, nations and military forces whose strategies have recognized and made best use of the current dominant technologies have prevailed in conflict. During the

Civil War, greater application of industrial technologies in the North gave Federal forces overwhelming advantage over their Confederate enemies. It was not until World War I, however, that the full impact of industrial warfare was made manifest with the introduction of machine guns, tanks, and aircraft on the battlefield in significant numbers. And again American industrial power was decisive.

During World War II, the Allied plan BODYGUARD guided a major campaign, an information war, that was a prototype of future conventional warfare. For the first time as an element of national and military strategy, human and other resources were assembled and put to the task of inventing computers, radar, and other information systems, and then of applying them--plus many more traditional information weapon systems--in new and imaginative ways to attack and cripple the enemy's C^3I system. The target was Hitler's ability to command.

Command is an information function. The modern staff, and the data processing and communication systems it relies on, performs important value-adding analysis and decision services to aid the commander. The entire C^3I system is essential to conducting modern warfare, and is, therefore, a critical target to be attacked and a vital resource to be defended.

In World War II, the information battle reached its culminating point in June 1944. As a result of BODYGUARD, an active disinformation and operational deception plan, Hitler failed to reinforce his defenses in Normandy because he was denied accurate, precise, and timely information upon which to

base his decisions.

BODYGUARD was a relatively primitive information campaign conducted by men and women developing doctrine and tactics as they went along. General Norman Schwartzkopf's strategy for DESERT STORM, on the other hand, was a very sophisticated application of information-warfare theory and technique. On 17 January 1991, Coalition forces opened the battle by blinding the enemy's sensors and degrading his ability to communicate and process data. A deception operation fixed Iraqi forces along the Kuwaiti coast. Coalition forces then moved to the west, knowing the enemy could not observe that movement, and the ground attack proceeded with total security and surprise.

At a micro level, the Coalition employed precision-guided munitions with great effect, munitions critically dependent on accurate, precise, and timely targeting data. Precision-guided munitions allow massing of overwhelming force at a precisely defined point. Their employment in the battle confirmed that the ability to locate a target implies the ability to destroy it.

DESERT STORM was a singularly one-sided conflict. The next major war between modern, technologically advanced societies will likely see the application of arrays of sophisticated information systems on both sides in both offensive and defensive postures. Therefore, the principles of information war must be integrated into the body of doctrine underlying United States force-development and force-employment strategies. The information war will be the center of gravity. It must be the focus of our effort and our energy.

CHAPTER II

THE OBJECTIVE

> Thus, what is of supreme importance in war is to attack the enemy's strategy.
>
> Sun Tzu

The objective of war is to apply overwhelming force against the enemy's ability to wage war while at the same time defending your own, and thereby force the enemy to your will. The Clausewitzian concept of the center of gravity refers to a critical focus of the conflict which is the key to victory or defeat. The side that controls the center of gravity is in an undeniable position to apply overwhelming force against the enemy. According to Clausewitz, the center of gravity is a product of the dominant characteristics of the two belligerents, a resultant of the interaction of the principal strengths and the principal weaknesses of each side. Each strength carries within it a weakness, a vulnerability.

In the current era, a major battlefield strength of technologically sophisticated modern forces is the ability to use precision-guided munitions. The weakness or vulnerability that strength carries with it is a critical dependence on being able to acquire accurate, precise, and timely targeting information. In a conflict between two modern forces, a center of gravity will

be the information sphere each struggles to dominate. In a conflict between two less well matched forces, the center of gravity may lie elsewhere, but it will still be bounded by the intersection of the dominant characteristics of the belligerents.[1]

The problem in war is twofold: First is to correctly identify the center of gravity, and second is to identify

---

[1]Clausewitz's concept of the center of gravity is generally misunderstood to be a critical target or operational objective. In fact, Clausewitz specifically identifies the critical target and operational objective to be the enemy's ability to wage war. The center of gravity is the focus of the conflict; it is itself a great battle, a struggle for dominance in a critical arena. Clausewitz writes, "Force--that is, physical force, for moral force has no existence save as expressed in the state and the law--is thus the means of war; to impose our will on the enemy is its object. To secure that object we must render the enemy powerless; and that, in theory, is the true aim of warfare." (p. 75) "The fighting forces must be destroyed: That is, they must be put in such a condition that they can no longer carry on the fight." (p. 90) "But in general it remains true that great battles are fought only to destroy the enemy's force, and that the destruction of these forces can be accomplished only by a major battle. The major battle is therefore to be regarded as concentrated war, as the center of gravity of the entire conflict or campaign." (p. 258) "What the theorist has to say here is this: one must keep the dominant characteristics of both belligerents in mind. Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed." (pp. 595-96) (Emphasis throughout in the original.) (Carl von Clausewitz, On War, ed. and trans. by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976)).

Strategy is the link between the means of war and its object. When two forces engage, the force-development strategies that shaped and characterized the forces and the employment strategies that deployed them on the field will determine the outcome of the contest. Thus, as Sun Tzu suggests, what is of supreme importance in war is to attack, and defeat, the enemy's strategy. (Sun Tzu, The Art of War, translated by Samuel B. Griffith (London: Oxford University Press, 1963), p. 77.)

operational objectives, clearly defined and attainable, which, when achieved, give us control of the center of gravity and permit us to destroy the enemy's will and ability to resist. Information warfare applies in two ways:

If an operational objective is destruction of a finite entity, then the problem becomes locating that target with necessary and sufficient accuracy and precision in space and time, so that a weapon can be brought to bear to destroy it. The second application of information war follows necessarily from the first. In order to destroy an enemy's ability to resist, it is sufficient that he be denied targeting information of the requisite accuracy, precision and timeliness, thereby preventing him from engaging you with his weapons.

While the foregoing statement may appear to be obvious, in fact it has been only in recent years that sensor, communication, and information-processing technologies have matured to the point that virtually the whole of the earth's land surface, the surrounding seas, and the air and space above are at least potentially subject to continuous, detailed surveillance. That degree of surveillance does not occur today because the sensors and their support systems, including the humans who attend them, are too expensive; because the quantity of data so produced would be overwhelming; and because it simply is not necessary. But large portions of the earth, sea, and sky are under nearly continuous observation (with the remainder subject to observation as required), and potential targets are monitored with very accurate and precise data being collected on their locations and

movements.

Not only does the technology now make targeting information available to a degree never before possible, but the weapons are now available to make use of the information. Accurate, precise and timely information is the sine qua non of precision-guided munitions. Whether the targeting sensor and precision-guidance mechanism are integral parts of tne weapon, are carried on the delivery platform, or operate from a third vehicle or location, the result is the same. Anything that can be located in time and space can be targeted and destroyed, and the only limitations on locating the target are the expense, effort, and time the attacker can accept in solving the problem.[2]

Given the required information, a decision may be made not to attack the target directly for policy reasons. For example, if the operational objective is destruction of a charismatic dictator, and if he is known to be in a survivable underground bunker, well supplied with life-support essentials and well defended, the only feasible direct attack against him may require the use of nuclear weapons. If the national command authority does not authorize the use of nuclear weapons, then an indirect

---

[2]Precision-guided munitions are the extreme case that dramatically demonstrates the relationship between targeting information and weapon. In fact, all weapon systems require targeting information of some degree of accuracy, precision, and timeliness. The difference is one only of degree. The opposite extreme to the precision-guided weapon might be a nuclear device detonated in an air burst to achieve an area effect.

attack will be necessary.

However, if the enemy knows you have the material capability of destroying him, and if he also believes you have the requisite will, he may be deterred from opposing you. Deterrence becomes a near certainty if he believes he lacks a countervailing capability. If he nonetheless chooses to fight, the engagement may be prosecuted to a successful conclusion if he in fact lacks either material capability or necessary and sufficient targeting information.

In the case of DESERT STORM, destroying the Iraqi information collection and distribution system made possible destruction of their material means of war without significant opposition. Lacking an information system, the Iraqi forces were unable to defend themselves. Exactly why Saddam Hussein was not deterred from resistance can only be the subject of conjecture.

CHAPTER III

THE OFFENSIVE

> The experts in defense conceal themselves as under the ninefold earth; those skilled in attack move as from above the ninefold heavens. Thus they are capable both of protecting themselves and of gaining a complete victory.
>
> Sun Tzu

Intelligence

Offensive capability in information warfare is intelligence. Military intelligence has two roles: Identify and assess the threat, and make target nominations. These two roles comprise an iterative process; repeating step one post-strike yields revised threat assessments which, in turn, yield new target nominations, and so on. [1]

---

[1] In this essay I use the term intelligence to describe a process of gathering information, processing and analyzing that information to reach certain conclusions about hostile or potentially hostile elements in the world, and then making recommendations about attacking or defending against those elements. Those are the essential functions of a unified command J-2, for example. Equally, identifying and assessing a threat may be a matter of milliseconds for a radar warning receiver (RWR) system in a modern war plane, and the pilot may complete the targeting process in the time it takes him to turn his head. The difference in time required to complete the process is not important; the intelligence process remains the same.

Identify and Assess the Threat

Identifying the threat is a process of collecting and analyzing information. In the beginning, at some notional time zero, sensors start collecting data about the world. Once collected, the data must be converted to a form compatible with follow-on analytical processes. That conversion may be as simple as developing and printing a photographic print, or as involved as resolving an electromagnetic signal into a series of characters, breaking a high-grade cipher system, and then translating the result into English. At this point the information can be analyzed in the context of any available historical data bases plus contemporaneous information from other sources to yield characterizations about objects and events observed. The first questions to be answered will be, What is it? Where is it? and When was it there?

It is easy to oversimplify the collection process. Successive iterations of employing sensors require an assessment of what additional data is required and where and how it might be found so that appropriate sensors can be brought to bear. The product continuously feeds back into the collection management system, where it is subjected to an analytical process to guide the collection of further data.

Threat assessment has two component parts:

1. Determine or estimate the enemy's material capability to wage war

2. Determine or estimate the enemy's intent to employ

that capability against you or your interests

Again, estimating enemy capabilities can be as simple as counting tanks in a marshalling yard, or as challenging as assessing characteristics of a developmental weapon system from partial intercepts of telemetry. Once again, both current situational data from one or many sources and historical data must be considered to reach conclusions.

Material capability is not measured in numbers of weapons alone, nor their deployment status, or the like. The critical question is what force the enemy can bring to bear within a specified time frame. To answer that question, numbers, locations and physical characteristics of weapons, training and readiness of enemy personnel, and the information capability that quickens the opposing force must all be considered. That is, can the enemy command and control his forces? Can he target you?

In terms of the information war, intelligence attack against the enemy's information system takes on special meaning and significance. All intelligence disciplines have roles to play, but signals intelligence (SIGINT) is the most immediately relevant because of its timeliness and generally inherent accuracy and reliability, and because the unique insight it gives into the enemy's C^3I system essentially turns his own information system into a weapon of self-destruction.

Compared to measuring material capability, assessing enemy intent approaches a black art, requiring nearly clairvoyant insight into the personality and mental processes of the enemy commander. Artificial intelligence techniques of expert systems

and pattern recognition may have application to this ancient problem and offer the prospect of developing into devastating new weapons of the information war.[2] Using such techniques, it may be possible to build a machine analog of an opposing commander that could be used to test for reactions to various courses of action.

Make Target Nominations

In order to make target nominations, two things are

---

[2]An expert system is a computer program with a knowledge base of expertise capable of reasoning at the level of an expert human in some given knowledge domain. Expertise is proficiency, the skill and knowledge humans use to perform tasks and solve problems. Expertise typically involves combining information with heuristic rules, rare facts, metaknowledge and metacognition, and compiled forms of behavior that yield skilled performance. (Raoul Smith, The Facts on File Dictionary of Artificial Intelligence (New York: Facts on File, 1989), p. 65.) Expert systems employ human knowledge in a machine environment to solve problems that normally require human intelligence. They simulate human performance in a specified knowledge domain and present a humanlike facade to the user. (F. Hayes-Roth, "Expert Systems," in Encyclopedia of Artificial Intelligence, ed. Stuart C. Shapiro (New York: John Wiley & Sons, Inc., 1987), pp. 287-8.) Pattern recognition systems automate a class of perceptual and cognitive processes, including processing raw data to derive patterns; determine if those patterns exhibit distinct characteristics for categorization and, if so, what categories those are; and assign the pattern to a defined category. (L. N. Kanal and G. R. Dattatreya, "Pattern Recognition," in Encyclopedia of Artificial Intelligence, p. 720.) Such patterns may be found in visual images, human speech, or a mosaic of events. Combining techniques of expert systems and pattern recognition, and perhaps other artificial intelligence techniques, might, for example, lead to a machine simulation of an individual leader's expertise applied in a specific event environment to yield a "most likely" prediction of that leader's response. Of course, if the leader in question is the enemy, capturing his expertise and identifying templates relevant to his pattern-driven behavior could also be massive tasks. The point is, such tasks are now merely very difficult, no longer impossible.

necessary: First, the potential target must have been identified, and it must have been located in space and time. Second, each potential target must be assessed according to two measures of merit: The degree of threat it poses to friendly forces and capabilities (negative value), and the utility in terms of achieving operational and strategic objectives of attacking the target (positive value).

The targeting process is completed with an assessment of vulnerability to specific weapons and the feasibility of attack. Here one crosses the line from intelligence to operational planning. As suggested earlier, at the current state of information technology, if a target can be located with necessary and sufficient accuracy and precision in space and time, a weapon can be brought to bear to destroy it. There remains only the policy decision of whether or not to do so.

Protect Your Own

Given an understanding of the offense in information war, it becomes possible to develop a defense. There are two essential steps in offensive information war. The first step is data collection, which can be defeated by counter-sensor strategies. The second step is a series of analytical processes. Strategies to attack the analytical processes are also possible. In order to target the enemy, it is necessary to complete both steps. In order to prevent successful targeting by the enemy, it is sufficient to defeat either of the two steps.

Stealth

Stealth is a passive counter-sensor strategy and consists of dramatically reducing observable features of the potential target, typically a combat vehicle. Observable features are those which emit or reflect energy detectable by human senses or machine sensors. The primitive ambusher might be considered the original stealth warrior.[3] The advent of stealth as an adjunct of modern warfare technique and technology, since it is specifically a technique of information warfare, is giving rise to whole new categories of doctrine and tactics that are significantly changing combat operations. Not least among those innovations is the realization that target survivability can be increased by signature reduction as well as by hardening. Communicating, traditionally considered essential for command and control, may gain greater tactical significance as a source of targeting data by revealing the location of the communicators.[4]

Active counter-sensor strategies

The enemy's ability to target can be physically destroyed ("hard kill"), or it can be degraded to the point of ineffectiveness by jamming, that is by overwhelming it with spurious data to the point that the system cannot locate targets with sufficient accuracy and precision ("soft kill"). Destroying or jamming communications links between sensors and the command

---

[3]Captain James Patton, USN (Retired), "Some Operational Implications of Stealth Warfare," Naval War College Review (Winter 1990), p. 67.

[4]Ibid., pp. 70-71.

and control nodes they support is a simple logical extension of these active counter-sensor strategies.

Deception

Deception is both a counter-sensor strategy and an attack against the analytical process which is integral to the C^3I system. It applies at all levels of conflict from national-strategic through small-unit tactical. It is a direct attack on the enemy with the objective of forcing upon him false data which will lead him to incorrect conclusions and bad decisions. A deception campaign will have three components:[5]

1. Concealment. Do not allow the enemy to locate, identify, and assess your capabilities, vulnerabilities, and intentions. Again, concealment may call for either active or passive measures, or both.

2. Deception proper. Mislead the enemy about those capabilities and vulnerabilities he does observe, and about your intentions for the future. It is a cardinal principle of deception that the deceiver succeeds by reinforcing the enemy's already formed misconceptions.[6]

3. Misdirection. Direct enemy attention to misleading or irrelevant data. A diversion succeeds by drawing attention away from the main effort, though perhaps for only a short time.

Example: At the successful culmination of BODYGUARD

---

[5]Eliot A. Cohen and John Gooch, Military Misfortunes (New York: The Free Press, 1990), p. 117.

[6]Ibid., p. 118.

in June 1944, the German ability to collect information had been severely degraded, allowing the Allies to conceal their capabilities and intentions. At the same time, false, deceptive and misleading information was introduced into the German C^3I system. Hitler was deceived into holding his 15th Army in reserve at the Pas de Calais, targeted against the notional First U.S. Army Group, instead of employing that army to oppose the Allied landings at Normandy. At the moment General Marshall and the other chiefs of staff learned of Hitler's decision, they knew ultimate victory was certain.[7]

Attacking the Analytical Process

Beyond denying or degrading current situational data by attacking sensors, the analytical capability can be attacked in two ways:

One possible mode of attack is to inject a virus into the computers performing automated analytical tasks, or degrade their performance by bombarding them with electromagnetic radiation. Attacks against human logical processes are possible by adding stress through increasing physical danger, hardship, deprivation, and isolation; increasing operational tempo to reduce decision time; etc. A bad decision is not necessarily an "intelligence failure." Information may be disregarded by the decision maker,

[7]Anthony Cave Brown, Bodyguard of Lies (New York: Harper & Row, Publishers, 1975), p. 687.

or his reasoning process may be faulty. Faulty reasoning may be induced as described.[8]

Mobility is a special case of increasing operational tempo. Mobility confers security on a potential target by shortening the time between establishing the target's location in space at a particular point in time and required arrival time of the weapon. That is, the more mobile the target in terms of its speed and agility, the shorter the time and distance by which we may "lead" the target. (The concepts of mobility and "leading" the target are discussed more fully in chapter V.)

The second possible attack on analytical capability requires a long-term effort to deny the enemy an accurate knowledge base of your capabilities, operational habits, and doctrine. Lacking an accurate knowledge base, the enemy will misread current situational data and, consequently, will make bad decisions.

> Example: Rommel, commanding the Atlantic Wall, believed the weather on 6 June 1944 would prevent an Allied amphibious operation, and so he went on leave back to Germany. In fact the Allies had superior weather information, allowing them to plan the attack for 6 June, because German weather data collection capabilities had been destroyed. Further, Rommel believed Allied forces would not attempt an amphibious

---

[8]Ole R. Holsti, Crisis, Escalation, War (Montreal: McGill-Queens University Press, 1972), pp. 199-200, 206-7.

operation if the waves in the English Channel were over six feet; in fact the Allies did not adhere to that doctrine on D-Day.

CHAPTER IV

MASS AND ECONOMY OF FORCE

> If I am able to determine the enemy's disposition while at the same time I conceal my own, then I can concentrate and he must divide. And if I concentrate while he divides, I can use my entire strength to attack a fraction of his.
>
> Sun Tzu

Information warfare is not confined to a traditional battlefield, even including the above- and below-surface extensions of the battlefield exploited by modern weapons. Identifying and understanding the Clausewitzian center of gravity requires an assessment of "the dominant characteristics of both belligerents." "Out of these characteristics a certain center of gravity develops, the hub of all power and movement, on which everything depends."[1] From comprehension of the center of gravity, employment strategies can be developed which, in turn, lead to operational objectives. The accurate, precise and timely identification of a critical threat, or reciprocally a critical target on the enemy's side, can be extremely difficult, but it is an information function at the heart of information warfare. Only after such an identification has been made can superior

---

[1]Clausewitz, pp. 595-96.

combat power be applied at the point of decision.

As weapons become smaller and fewer, the requirement for accurate, precise, and timely targeting data becomes greater. The weapons are smaller, but they deliver more force to a more precisely defined point than ever before. The GAU-8 30mm cannon carried on the A-10 attack fighter destroys a modern tank with a slug of depleted uranium measuring approximately one inch in diameter by about four inches long. A similar slug of depleted uranium protected against the friction and heat of reentry dropped from earth-orbit altitude would carry sufficient energy to penetrate the most hardened nuclear missile silo. The critical problems to be solved are locating the target and then guiding the weapon to that target. If the target is mobile, the problem is more complex, but not different in any essential way. Depleted uranium is the material of choice, of course, because of its mass density. As a weapon it approaches a theoretically ultimate expression of the principle of mass.

The reciprocal of the principle of mass, economy of force requires that threats and potential targets be accurately assessed to ensure that scarce combat resources are not wastefully expended against enemy deceptions or in other, secondary, efforts. Again, the weight of effort and responsibility is on the information system. Modern weapons are fewer in number and more expensive than their forebears. Even worse than suboptimally expending them in secondary efforts is wasting them blindly with no clearly defined or located target.

CHAPTER V

MANEUVER

> And as water has no constant form, there are in war no constant conditions. Thus, one able to gain the victory by modifying his tactics in accordance with the enemy situation may be said to be divine.
>
> Sun Tzu

In traditional analysis, maneuver includes the interrelated dimensions of flexibility in thought, plans, and operations, and the mobility necessary to mass combat power at the point of decision.[1] In terms of information warfare, flexibility of thought and action translates to rapidity of decision making and action in the face of new and changing data.

The target must be located in both time and space. Time is a vector quantity,[2] and the target's location in space must

---

[1]Headquarters, Department of the Army, FM 100-5: Operations (5 May 1986), p. 175.

[2]A vector is a quantity of a type that might be represented by a directed line segment having magnitude and direction. In time, magnitude is expressed in units of seconds, minutes, hours, days, etc. Direction of movement is indicated by what Steven Hawking calls "time arrows." (Steven W. Hawking, A Brief History of Time (New York: Bantam Books, 1988), pp. 143-54.) Of particular interest here is the thermodynamic arrow of time, which points in the direction of increasing entropy. Entropy is a measure of the disorder of the universe. It is also a measure of information content such that increasing entropy equates to increasing information content. In this context,

be expected to change over time. The relevant time period over which accurate predictions of spatial location must be made is the time required to make a decision to engage the target plus the time required for the weapon to close on the target. Security for the target equates to a degree of mobility, speed, and agility that takes it beyond the radius of the weapon effect faster than the enemy can react.

> Example: At one extreme, a duck hunter leads his target by feet and fractions of a second. At the opposite extreme, the United States maintains constant surveillance and intelligence collection efforts against the Soviet Union while strategic forces are kept on alert. We "lead the target" by time equal to the time required to transmit data from strategic sensors to the national command authority (NCA), plus NCA decision time, plus time required to launch

---

information can be defined as the unpredictable elements of a signal. Thus, the arrow of time points in the direction of increasing information, and in the direction of increasing uncertainty (unpredictability). In terms of this essay, that uncertainty may be visualized by considering a target such as an enemy aircraft in flight. The target may be observed and its location determined at a given point in time, but with each passing increment of time the target's location will become increasingly uncertain until or unless additional observations are made. Of course, if that observation must be communicated to a higher command echelon, and if analytical processes must be applied before a decision is made or action is taken, then all concerned must know and understand that the data they are dealing with come with a certain amount of built-in uncertainty. The commander must decide if the cost of additional uncertainty is compensated for by the benefit of the value-additive services of his information system.

weapons, plus flight time of the weapons to their targets.

The acknowledged strengths of air power--speed, range, flexibility, precision, and lethality--reflect its ability to react rapidly to targeting data that may be valid for only a short period of time. That is, a fast-moving airborne weapons platform can strike a maneuvering target if the target's location is known or can be predicted (extrapolated) within acceptable limits of accuracy and precision over the time required for the aircraft to bring its weapons within range and launch them. That time becomes shorter as the distance to be covered lessens, and the requirement for prediction lessens as the time decreases. Thus an aircraft orbiting over the battlefield has greater utility against a target of opportunity than one back at home base, and forward deployed forces in general have less stringent target-information requirements than those in rear-area garrisons.

The acknowledged value and importance of air power in modern warfare comes from the ability of the crew of a manned aircraft to collect, process and exploit targeting information at real time and to deliver large weapon loads rapidly with relative precision and accuracy. Over the past 75 years aircraft have come to dominate the battlefield because of these characteristics, and their strengths have only been enhanced as information technology has improved. As information technology continues to mature over the next 75 years, however, we may find other ways to acquire targets and deliver weapons quickly to

them. One possibility among many might be a cruise missile with a conventional warhead guided to its target by a spaceborne sensor and the Global Positioning System (GPS/NAVSTAR). Or consider as a solution to the infantry's requirement for close air support a soldier providing targeting information to a cruise missile through a combination of laser target-designator and GPS/NAVSTAR precise-location information. Real-time or near real-time information processing remains the critical element and may or may not involve a human in the loop at an unspecified location.

The debate over the militarization of space is fatuous. The presence in earth orbit of such information systems as intelligence sensors, communications satellites, and GPS/NAVSTAR has effectively militarized the region. The only issue is whether destructive weapons will be placed in orbit also to permit more rapid reaction to volatile targeting data on a terrestrial, airborne, or space-based threat. The stated U.S. goal of an ASAT capability, not necessarily in space, is a recognition of the information warfare capabilities of spaceborne systems.

CHAPTER VI

UNITY OF COMMAND

> Generally, management of many is the same as management of few. It is a matter of organization. And to control many is the same as to control few. This is a matter of formations and signals. Thus the valiant shall not advance alone, nor shall the coward flee.
>
> Sun Tzu

Alexander to Napoleon

Command is an information function. The quantity of data available and the speed of information transfer have increased exponentially over the course of human history, but the basic information-processing device employed by military commanders has not changed since the days of Alexander the Great. That device is the human brain. But over the course of history, commanders have developed a variety of techniques to assist them with their information-processing requirements. The first major advance over Alexander came in the eighteenth century with the development of the military staff. Napoleon Bonaparte was the first to command a multi-corps army in the field through a general staff headed by a chief of staff. Napoleon's staff received reports from counterpart elements on the staffs of his subordinate field marshals and issued instructions in his name. All quite routine in today's vast military bureaucracies, in 1800

it was revolutionary. And it was key to Napoleon's success.[1]

The headquarters staff developed to take the communications and data-handling load off the commander. The eighteenth century commander, however, did all his own intelligence analysis and operations planning; he had a staff, not the modern staff method.

The Modern Staff Method

Reduced to simplest terms, a staff is an information-processing device. Properly conceived and implemented, the modern staff method further relieves the commander of information-processing duties by having the staff subject incoming information to a value-adding analytical and parsing process. Decisions which can be made at levels below the commander are, in fact, made for him so that he has more time for analysis and decision making that only he can perform. The distinction of what is or is not within the purview of the staff is ultimately decided by the commander on the basis of his ability to "program" the staff to act as he would in its place, that is, the degree to which he can predict the nature of the problems it will have to solve and the degree to which he can make his intent known in advance. Trust in subordinates derives from experience which tells the commander that through whatever process and mechanism, the staff is appropriately "programmed." The value added to

---

[1]Martin Van Creveld, Command in War (Cambridge, MA: Harvard University Press, 1985), pp. 58-102.

information is measured in terms of utility of the staff product to the commander. That utility is measured in terms of timeliness and how readily the information can be accepted and used by the commander's decision making process. When the information is presented to the commander, he makes a decision which gives rise to orders to subordinate elements. That decision and the ensuing orders in turn become new information subjected to yet another value-additive, analysis-decision process as they are transmitted to the executing units.

Communications

The key and indispensable requirement for command is communications. Modern military forces are driven to seek security in dispersion and mobility. "The price or cost is the need of capabilities for fusing, integrating, coordinating and ensuring the consistency of decisions and information across such geographically and logically dispersed entities as data bases, sensors, management levels, organizations and knowledge domains."[2]

The down side to communications is twofold: First the communication system or its output signals may be observable, and either feature may identify to the enemy a critical node in a C^3I network or an otherwise stealthy weapon, platform, or

---

[2]Albert J. Baciocco Jr, Rear Admiral, USN, "Artificial Intelligence and C^3I," in Applications in Artificial Intelligence, ed. Stephen J. Andriole (Princeton, NJ: 1985), p. 498.

operator. Second, it puts the information at risk at the same time it is gaining value through increased utility. That is, while the information is in motion it can be intercepted and exploited, or it can be degraded or destroyed by electronic combat techniques.

> Example: At the time of the Normandy invasion, the Allied command ordered French resistance forces to destroy telephone exchanges used by German command authorities. The immediate result was only a temporary disruption to German command and control; they quickly reverted to radio communications. That change, however, made German command information available for intercept by the Allies. Since the Allies, unknown to the Germans, had broken the highest level German operational cipher system through the ULTRA program, what at first appeared to be a harassing action by resistance forces became an important attack on the enemy's information system.

Unity of Command

Unity of command means that an entire organization is guided by the intent of a single commander. This unity ensures that all elements of the organization have the benefit of all information and information-processing capability available to the commander without having to duplicate either the information or the processing capability at all echelons. The implied requirement is that the commander have reliable and secure communications to transmit his intent and orders, the product of

his information system, to those subordinate elements. Equally, the subordinates must be able to use the commander's intent as a guiding model or framework within which to develop courses of action based on new or unexpected information arising from a changing tactical situation.

In the United States military, the tactical employment of forces is led by captains, majors and lieutenant colonels for the most part. These leaders at the squadron-battalion level today are absolutely dependent on targeting and other intelligence from higher echelon analytical centers.[3] Modern telecommunication and microcomputer technologies make possible distributed information processing which reduces dependence on a centralized capability. These technologies support "low-abstraction" tasks well; they are less useful in situations calling for nonroutine, innovative problem solving.[4] Mission planning is one such

---

[3]The range of information services routinely provided by "higher headquarters" is immense, including such essentials as air space management, deconfliction of maneuver and indirect fires, frequency management, etc. In the specific realm of intelligence analysis and fusion, it is a fact of life that these centers are most often found at flag-officer-level headquarters, far from the executing forces.

[4]Alvin Toffler, The Third Wave (New York: William Morrow and Company, Inc, 1980), pp. 213-16. Toffler's examples of "low-abstraction" tasks include "entering data, typing, retrieving, totaling columns of figures . . . and the like." (p. 213) This list of tasks describes much of what happens in the principal intelligence agencies and major headquarters of modern defense establishments. Such tasks do not, in general, involve a great deal of creative thought, nor do they require face-to-face transactions. By contrast, innovative problem solving tasks are highly creative and are greatly enhanced by direct interpersonal communication with all the subliminal and nonverbal information transfer it entails. The results of well orchestrated team problem solving and innovation are generally superior to any

nonroutine situation. The Chief of Staff of the Air Force has proposed an innovative organization for air forces, a composite wing structure similar to the Navy's carrier air wing, to bring together the people who need face-to-face communication for nonstandard information exchange.[5] Less critical, readily formatted communication is left to electronic means. The critical elements requiring personal interaction are intelligence and operational planning.

The commander's intent and orders, therefore, are his most important product, embodying as they do the sum of his understanding of the center of gravity, his knowledge of the enemy and the situation, his designation of critical targets, and his predictions about future tactical situations. All of these are essential to the operation of modern forces, and the value of information-based processes explains why a C^3I system is a critical target to be attacked, and a vital resource to be defended.

---

individual effort. The principal limiting factor in data transfer by electrical means is channel bandwidth. Human beings are wonderfully efficient packages of data storage and information processing capability, and there are times when the most efficient means of transferring information is by bringing two or more people together, even if long distances must be covered.

[5]General Merrill A. McPeak, USAF, "For the Composite Wing," Airpower Journal (Fall 1990), pp. 4-12.

CHAPTER VII

SECURITY AND SURPRISE

> If plans relating to secret operations are prematurely divulged, the agent and all those to whom he spoke of them shall be put to death.
>
> Sun Tzu

If the enemy cannot gain accurate, precise, and timely information about you upon which to base his plans and with which to target his weapons, he will have been denied the ability to wage war against you. That is the definition of security, and is the Clausewitzian definition of victory.[1]

Surprise, the reciprocal of security, is the result of victory of your information system over that of the enemy. The requirements for surprise are that you be able to target the enemy at a time and place and in a manner that he does not expect. That is, you have capability that he has not discerned and intent he has not discovered, while at the same time your intelligence capability has identified and located a lucrative target that is within your capability to strike.

If while you are denying the enemy the ability to target you, you still can target him, your advantage is absolute and

---

[1]Clausewitz, p. 90.

undeniable. This condition is precisely what the Coalition commander achieved in DESERT STORM. It is also the same logic which makes the Strategic Defense Initiative seem so very threatening to the Soviet leadership, though in this case denial of targeting ability becomes a factor in the endgame rather than at the opening.

CHAPTER VIII

SIMPLICITY

The state of crisis is the real war.

Carl von Clausewitz

Crisis is defined by time constrained high-stakes competitive information processing and decision making. Typically, time is short, the amount of information to be communicated and analyzed is large, and the attendant stress tends to degrade human logical processes. At such times the degree to which the problem can be simplified, that is the degree to which the analytical requirement can be reduced, equates to a material advantage in the competition.

In war the decision will be reached through combat. There is no more stressful human condition. Time for thought and analytical capability are at a minimum. Unity of effort and coherent implementation of the commander's plan and intent are critical. Since it is said no plan survives contact with the enemy, engaged forces will have to improvise on the theme of the commander's intent. Under such conditions, there is a premium on simplicity to reduce the analytical and decision-making workload.

Simplicity is relative to the availability of information-processing capability. There is a temptation to advocate widespread use of artificial intelligence devices to augment the

tactical commander, and certainly such devices will have a place on tomorrow's battlefield. However, care is essential to ensure that tomorrow's leader is not overly dependent on such aids, or upon any single source of information, lest he be completely disabled by their failure at a critical moment.

CHAPTER IX

SOME IMPLICATIONS

Carl von Clausewitz would not have liked this essay. For him intelligence was part of the fog and friction of war.[1] Surprise was important but overrated, deception and cunning were all too often employed at the expense of more essential qualities of character, and an indirect attack on the enemy, that is anything other than "direct annihilation of the enemy's forces," was an undesirable distraction from what should be the "dominant consideration."[2] But even Clausewitz recognized that changes in technology and technique would bring about changes in strategy,[3] and that has been the thesis of this essay.

At this writing, the Soviet Union is the only country which can still seriously challenge the United States in the

---

[1]Clausewitz, pp. 117-18. "This difficulty of accurate recognition constitutes one of the most serious sources of friction in war, by making things appear entirely different from what one had expected." (Emphasis in the original.) Exactly. Intelligence has matured to a high art only in the twentieth century, and the high technology which serves that art has become available only in recent years. Clausewitz was correct for his time, and the "difficulty of accurate recognition" remains, but our ability to solve that difficulty far exceeds anything the old master could have imagined.

[2]Ibid., pp. 198, 202-3, 228.

[3]Ibid., p. 226.

strategic military arena. That challenge is serious only because of the Soviet strategic nuclear missile arsenal, weapons of mass destruction whose targets have long been known and precisely and accurately located. The Soviet base of information technology and industry cannot compete with that of the United States. The performance of Soviet weapons against U.S. weapons--most recently in DESERT STORM, but also in other conflicts--confirms that. It may be too late to try to hide certain fixed strategic targets within the United States, but in any conflict short of nuclear war (and perhaps even then) the superiority of U.S. information warfare capability must prove decisive.

Clearly, the ideas discussed in this essay have greater application to conventional rather than strategic nuclear war. General Schwartzkopf's discussion of his campaign plan carried on CNN on 27 February 1991 was as concise and articulate a description of the current state of information war as could be wished for.

Other analysts have noted and commented on the emerging dominance of information technologies in war, with the added observation that the chief potential rival to the United States in this arena is not the Soviet Union, but Japan. Michael Nacht has said that the sinews of military power are the technologies that are Japan's strength: electronics, sensors, etc. While Japanese industry has the capacity to challenge the U.S., it currently lags in types and quality of military technology where

the U.S. holds an important lead.[4] Japan produces 52 percent of the world's semiconductors, and 21 major U.S. weapon systems contain semiconductors produced only by overseas manufacturers.[5] Japan is not going to become a major military power in the near future, but she clearly has the industrial base to do so at some time, just as her industry is the base of potentially far-reaching economic strategies. The United States can develop a fully self-sufficient defense industry only by first developing a self-sufficient electronics industry.

In the seventeenth and eighteenth centuries, the dominant considerations in warfare were the reciprocal concepts of position (especially of fixed fortifications) and maneuver. Battles in that era often consisted of a series of maneuvers, sometimes lasting for several days, leading to a final position in which the outcome of the armed engagement was inescapably determined. Under such conditions, the battle was often not taken to completion, and surrender was offered on the basis of victory or defeat in the position contest alone.[6]

---

[4]Michael Nacht, Dean of the School of Public Affairs, University of Maryland. Dr Nacht was speaking at the National Defense University symposium on Pacific security affairs in Honolulu on 2 March 1991. Cited by permission.

[5]Wendy Hanamura reporting on "Monitor Radio," the broadcast service of the Christian Science Monitor, 6 March 1991. Ms Hanamura cites as examples the M1A1 tank, and the TOMAHAWK and PATRIOT missiles.

[6]John Childs, Armies and Warfare in Europe 1648-1789 (New York: Holmes and Meier Publishers, 1982), pp. 101-5. "Destruction of the opposing army was not a general's main goal, rather he was under orders to manoeuver for particular areas and strong-points in an effort to seize them for political ends."

Clearly we have not yet reached an equivalent level of recognition of the importance of the information battle in modern conflict, nor are we likely to. It is difficult to imagine that a national government still possessing weapons--albeit apparently useless--will surrender without having actually experienced the futility of resistance. Deciding when continued resistance constitutes a last desperate bid for glory and when it is futile sacrifice requires a wisdom not shaped by "an airy formula."[7]

The struggle in the information sphere as described in this essay may not achieve the decision alone, but it will be decisive. A fundamental policy prescription is, therefore, in order.

The principles of information war must see specific application in United States force-development strategies, and they must be integrated into the body of doctrine underlying our force-employment strategies. To date there have been no deliberate, comprehensive studies of information-support structures of military forces with the intent of identifying all the critical vulnerabilities they contain. Nor has there been a comprehensive effort to develop weapons and tactics to attack (or defend) those vital structures beyond the lowest echelons of tactical sensors and communications.[8] Simply pursuing as an

---

(p. 104) See also Clausewitz, pp. 258-62. "Recent history has scattered such nonsense to the winds." (p. 259)

[7]Bernard Brodie, "A Guide to the Reading of On War," in Clausewitz, On War, p. 692.

[8]There is a notable exception in the area of

article of faith the high-technology solution in weapons research, development, and procurement will not be sufficient. Nor, in combat, is it sufficient to target the enemy's C^3I system as a secondary effort to destroying his armed forces. Information war will be central to future conflicts; it will be the center of gravity. Therefore, it demands our attention, our energy, and our best intellectual effort.

---

communications intelligence (COMINT) and its counterpart, communications security (COMSEC). Successes in these fields only suggest what might be possible with a more comprehensive and aggressive approach to the many aspects of the information war.

SELECTED BIBLIOGRAPHY

Andriole, Stephen J., ed. Applications in Artificial Intelligence. Princeton, NJ: Petrocelli Books, Inc., 1985.

Blahut, Richard E. Principles and Practice of Information Theory. Reading, MA: Addison-Wesley Publishing, 1987.

Brown, Anthony Cave. Bodyguard of Lies. New York: Harper & Row, Publishers, 1975.

Childs, John. Armies and Warfare in Europe 1648-1789. New York: Holmes and Meier Publishers, 1982.

Clausewitz, Carl von. On War. Translated and edited by Michael Howard and Peter Paret, with a commentary by Bernard Brodie. Princeton, NJ: Princeton University Press, 1976.

Cohen, Eliot A., and Gooch, John. Military Misfortunes. New York: The Free Press, 1990.

Hawking, Stephen W. A Brief History of Time. New York: Bantam Books, Inc., 1988.

Headquarters, Department of the Army. FM 100-5: Operations. 5 May 1986.

Holsti, Ole R. Crisis, Escalation, War. Montreal: McGill-Queens University Press, 1972.

Knorr, Klaus, ed. Power, Strategy, and Security. Princeton, NJ: Princeton University Press, 1983.

McPeak, Merrill A., General, USAF. "For the Composite Wing." Airpower Journal (Fall 1990), pp. 4-12.

Paschall, Rod. LIC 2010: Special Operations & Unconventional Warfare in the Next Century. McLean, VA: Pergamon-Brassey's, 1990.

Patton, James, Captain, USN (Retired). "Some Operational Implications of Stealth Warfare." Naval War College Review (Winter 1990), pp. 67-72.

Shannon, Claude E. "A Mathematical Theory of Communication." The Bell System Technical Journal (July 1948), pp. 379-423.

Smith, Perry M., Major General, USAF (Retired). "Air Battle 2000 in the NATO Alliance: Exploiting Conceptual and Technological Advances." Airpower Journal (Winter 1987-88), pp. 4-15.

Sun Tzu. The Art of War. Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

Toffler, Alvin. The Third Wave. New York: William Morrow and Company, Inc., 1980.

Van Creveld. Command in War. Cambridge, MA: Harvard University Press, 1985.

Warden, John A. III. The Air Campaign. Washington, DC: National Defense University Press, 1988.